Security of m-learning System: A Collective Responsibility

http://dx.doi.org/10.3991/ijim.v9i3.4475

S.A. Shonola and M.S. Joy
University of Warwick, Coventry, United Kingdom

***Abstract*—Innovation in learning technologies and services is driven by demands from Higher Educational Institutions (HEIs) in order to meet students' needs and make knowledge delivery easier. The technology could play a pivotal role in extending the possibilities for teaching, learning, and research in educational institutions. M-learning emerged from this innovation as a result of an unprecedented explosion in the number of mobile devices due to availability and affordability of mobile phones, smartphones and tablets among students. Competition in the mobile device industry is also encouraging developers to be innovative, constantly striving to introduce new features. Consequently, newer sources of risks are being introduced in the mobile computing paradigm at manufacturing level. Similarly, many m-learning promoters and developers focus on developing and delivering learning content and infrastructure for m-learning system without adequate consideration for security of stakeholders' data, whereas the use of these mobile technologies for learning poses a serious threat to confidentiality, integrity and privacy of those involved in teaching and learning, yet traditional security threats are also evolving. Against this backdrop, the stakeholders in education sector (i.e. education providers, educators, m-learning promoters and developers) should begin to consider the security implications of these devices in modern teaching and learning environments. The purpose of this paper is to identify the m-learning security issues that stakeholders may face, how they are being affected by these security threats, who among the stakeholders are affected or most affected by security issues in m-learning using three Nigeria universities as case studies and what are the responsibilities of the stakeholders in ensuring risk free m-learning.**

***Index Terms*—mobile learning security, m-learning security, security threats**

I. INTRODUCTION

M-learning is creating a new environment for teaching, learning and education delivery. It is a mobile-based learning process using internet technology to design, implement, select, manage, support and extend knowledge acquisition. As m-learning has many advantages such as flexibility and diversity, it has become a way of learning that augment classroom and e-learning. It is a growing trend that extends learning beyond lecture theatres and can be exploited to respond to the challenges of particular educational contexts, complement and enhance formal schooling, improve and assist learning for people of different ages and augment learning opportunities in communities where educational opportunities are limited. The development and adoption rate of mobile technologies are increasing rapidly on a global scale, many education institutions have aligned their curricula to accommodate m-learning and have invested in hardware and software resources to take full advantage of the new invention. There are numerous applications for mobile technologies in education, from the ability to wirelessly transmit learning modules and administrative data, to enabling learners to communicate with instructors and peers "on-the-go". Lecturers can give out lecture notes and instructions while on the move and students can listen to recorded lectures either online or offline anytime anywhere [1].

However, along with opportunities in m-learning come several challenges that need to be addressed. For instance, in an m-learning environment, educational materials and instructions can be passed to students through their mobile devices, but this adds another layer to the personal computer-based model of teaching and e-learning. Similarly, the pervasive use of m-learning may entail, among others, loss of privacy and attacks on users and institutional security. One important concern about the use of mobile devices in learning is the security risk and vulnerability issue relating to educational content and private information of stakeholders [2]. Higher Education Institution management, educators, and individual learners are profoundly worried about the growing security threats in m-learning. Concern about data security and privacy issues seems to be quite high among educators, education providers, m-learning developers and other stakeholders. Some perceived risks include unauthorised interference with the learning content and instructions by the learners. More importantly, as students are allowed to use their portable devices to access learning content and materials anywhere, this increases the security risks. Therefore, one security challenge is to ensure that students' have access only to their required learning material and instruction regardless of whether they learn in the lecture room or outside the classroom [3]. This paper specifically examines the collective responsibilities of stakeholders in ensuring risk-free m-learning environments.

This paper is an extension of work on Mobile Learning Security Concerns from University Students' Perspectives, reported in proceedings of the International Conference on Interactive Mobile Communication Technologies and Learning [4]. The original paper identified the security threats that students may face when using mobile devices for educational purposes and examined the perceived damaging effects of mobile learning on students in case there is a security breach. We extend our previous work by investigating the security threats which other stakeholders such as educational institution management, academic and support staff may face and discuss the collective responsibilities of the stakeholders in ensuring threat and risk free m-learning environment.

Our paper is organised as follows. The second section of this article is a review of related research on m-learning security. It summarises an existing study on m-learning security and evaluates the recommendations made in the literature. The third part discusses the research carried out on how security issues affect the use of m-learning (using three universities in Nigeria as a case study) from stakeholders' perspective, and who are responsible for ensuring risk free m-learning. It details the purpose of the research, the methodology and research questions. A brief overview of the analysis of the results of the research is presented in section four while section five gives a detailed discussion of the results gathered and statistical tests. The last part of this article highlights and discusses recommendations given to the security issues mentioned in the previous sections. The article concludes with problems encountered during the research and direction for future work in ensuring risk free m-learning environments.

II. LITERATURE REVIEW

In recent years there are many studies on mobile learning in academics institutions, although most of the studies are related to the development of mobile learning materials. Studies on the perception of stakeholders towards mobile learning security are few in number, and are examined in this section.

Guo et al. [5] observed that more academic institutions plan to integrate mobile security into their computing curriculum and found out that there are at least two challenges. The first challenge is the unique characteristics of mobile security, which is a new and evolving paradigm. Traditional security threats, such as malware or social engineering, are growing in this new environment using new attack vectors or adapting to the new platform. Similarly new components such as Global Positioning System (GPS) and services in mobile platforms introduce new sources of risks and few security courses cover the full spectrum of mobile security, especially those new and unique threats. The second challenge is the shortage of effective learning materials, compared to the rich learning materials available for general computer security or other special security areas such as web security or network security. Therefore, there is a need to explore a learning approach to mobile security from the perspectives of mobile devices (smartphones and tablets) and mobile applications (apps).

Charlesworth [6] stated that the use of mobile technologies poses a risk to the confidentiality, integrity and privacy of the data involved in the educational process for both the users and the services. The challenge, therefore, has to do with securing the systems and deploying proper security policies and procedures so as to be able to deter and repel attacks. It also requires insuring the integrity, privacy and confidentiality of the data stored and transferred for the needs of the educational process. Therefore, the provision of robust mechanisms to support user authentication, authorisation and non-repudiation, management of data, content copying, editing and downloading, safeguarding learner examination and assessment processes from attackers and impostors are some prerequisites for secure online learning arena.

Kamba [7] found out that some universities in Nigeria have websites and engage in m-learning for advertisement and information dissemination only and not for leaning purposes for various reasons, one of which is the security aspect. There are perceived risks, as such students interfering with the learning contents and instructions given to them by their lecturers and instructors. The security need in an m-learning platform is to protect the content, services and the personal data of the stakeholders and guarantee their confidentiality at all times [8]. In some cases, especially if the learning institution supplies learners with special mobile equipment, there exist worries about making them attractive to thieves. A key concern for educationalists and policy makers is ensuring that learners can use mobile technologies, and the online services and communication accessed through these technologies safely.

While the use of mobile technologies for academic purposes does not increase the risk that may already exist as a result of learners' personal ownership of mobiles, the designers and practitioners of education are, however, responsible for producing coherent and reliable accounts of the likely consequences of the proliferation of mobile devices in the higher education landscape [9]. The focus of this paper is on the challenges associated with mobile security specifically related to education sector stakeholders' concerns in the areas of safeguarding and protecting the privacy and security of individuals, data, systems and equipment. The outcomes of this research will contribute to the field of study in determining how various stakeholders in academic institutions are affected by the security issues in m-learning and in making recommendations for ensuring risk free m-learning environments.

A. Research Questions

This study attempts to answer the following questions:

1. What are the m-learning security issues that stakeholders may face?
2. How are the stakeholders in academic institutions being affected by the security threats in m-learning?
3. Who among the stakeholders are most affected by the security issues?
4. What are the responsibilities of the stakeholders in ensuring risk free m-learning?

III. METHODOLOGY

In identifying the challenges of m-learning security, two separate research activities were carried out as primary instruments to gather data. The first was an online and hard-copy questionnaire for collecting quantitative data from stakeholders, mostly the lecturers and learners who are the main users of m-learning. The second instrument was a series of interview with a sample of academic and support staff to obtain qualitative data on their observations and experiences on m-learning as well as their understanding of factors contributing to security threats in m-learning. The research study was conducted at three universities from South West Nigeria using qualifying demographics. Technical terms and concepts were explained in brief in the questionnaire and the researcher was available during the study to assist the respondents in understanding any part of the questionnaire. A total of 150 responses were gathered comprising of 120 questionnaire data and 30 interview responses, all of which were analysed. Secondary instruments for data collection are documented evidence, articles obtained from the academics

and administrative staff as well as information obtained through research papers from relevant journals which were used to support the primary data gathered from the research study.

IV. FINDINGS

The findings of this work are organised into three sections in order to provide answers to the research questions as shown below:

Research Question 1: What are the m-learning security issues that stakeholders may face?

The research question is a multi-choice question to find out various security issues stakeholders might have encountered when using mobile devices to complement teaching and learning activities. Fig 1.shows the various security issues, topping the list is unauthorised access to learning content and materials (75.6%), followed by virus/malware attack on m-learning system (68%). Denial of service is considered the least threat to m-learning system (30.5%).

Research Question 2: How are the stakeholders in academic institutions being affected by the security threats in m-learning?

This section addresses how security issues in m-learning affect the stakeholders i.e. the education institutions, lecturers/faculty members and the learners in case of security breaches.

Educational Institution Management/Promoters: This part of the survey investigated the adverse security effects of m-learning on the HEIs who are interesting in incorporating m-learning in their curriculum. Educational institutions and their management are stakeholders in knowledge development and delivery and they risk suffering loss of confidential information, reliability, and goodwill as well as working hours of the developers and support staff to security issues as shown from the survey data. Around nine out of ten participants (87.78%) indicated loss of confidential information as the most adverse effect of security threat to m-learning for HEIs. Eight out of ten participants indicated loss of goodwill and integrity as the risk of m-learning threats to the HEIs. In case of successful hacking, there is a loss of reliability on the part of the institution which 77.8% of the respondents pointed out. 43.3% of respondents also perceived loss of working hours in correcting the anomalies, restoring students' confidence and rebuilding integrity of the institution after a security breach.

Academic/support staff: The educators may risk loss of confidential information, unauthorised change in learning content, loss of control during e-examinations, loss of privacy as well as psychological effect. From Fig. 3 below, around nine out of ten participants (93.3%) indicated that loss of confidential information is a major consequence of the m-learning security threat to educators while more than eight out of ten participants (86.67%) were of the view that loss of control mainly during e-assessment and online examinations is a threat to the academic staff. Also more than eight out of ten (83.3%) agreed that loss of content quality of learning materials is a concern while exactly three out of ten indicated psychological effects as a consequential result of m-learning security threats. Almost half of the participants (48%) are of the view that loss of privacy is a security threat to m-learning for the academics.

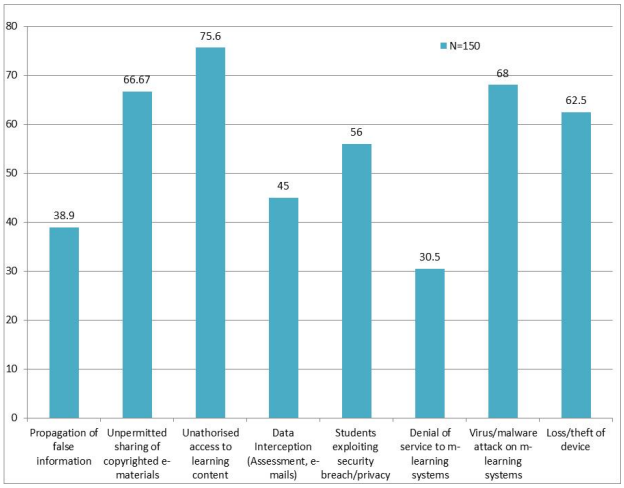

Figure 1. What are the m-learning security issues that stakeholders may face?

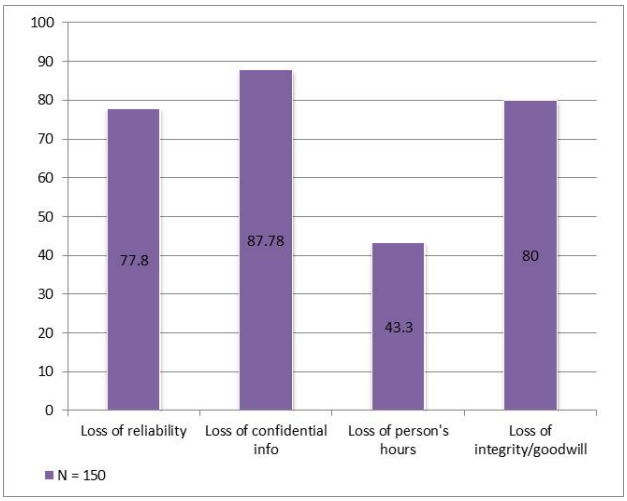

Figure 2. How the stakeholders (HEIs Management/ Developers) are affected by m-learning security threats

Students: Being one of the stakeholders in m-learning are exposed to the following risks as gathered from participants in the research study: loss of performance (65%), loss of study hours (71.67%) and loss of their confidential information (80%) as well as psychological effects (46.67%) as shown in Fig. 4 below.

Research Question 3: Who among the stakeholders are most affected by the security issues?

This section of the study reveals that among the different stakeholders in a university community, the university management are most affected by any security threats. The faculty lecturers and students as users are also affected next, after the management. Fig. 4 indicates that the vast majority of respondents (66.67%) indicated that the university management and promoters are most affected by m-learning security threats among all the stakeholders. This is highly likely to happen as they are the policy makers in charge of the smooth running of the university. The lecturers and support staff are next as perceived by 53.33% of the participants. Students are affected as indicated by four out of ten participants. The developers are least affected if the m-learning systems are being developed by consultancy outfit or software company as found out in the research study.

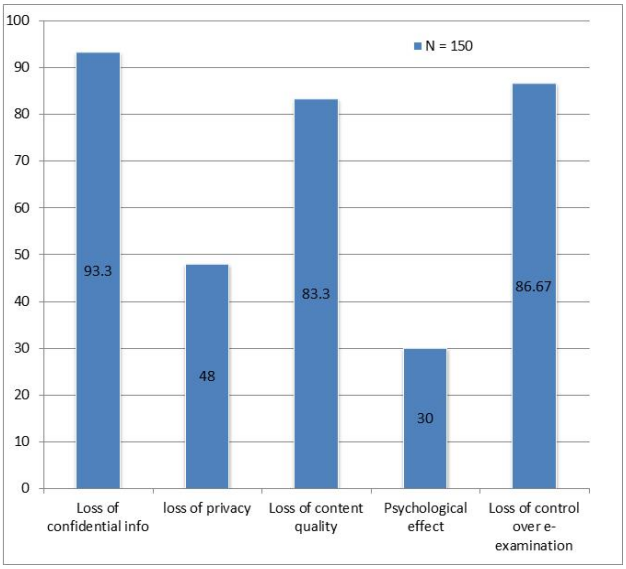

Figure 3. How the stakeholders (Academic/support staff) are affected by m-learning security threats

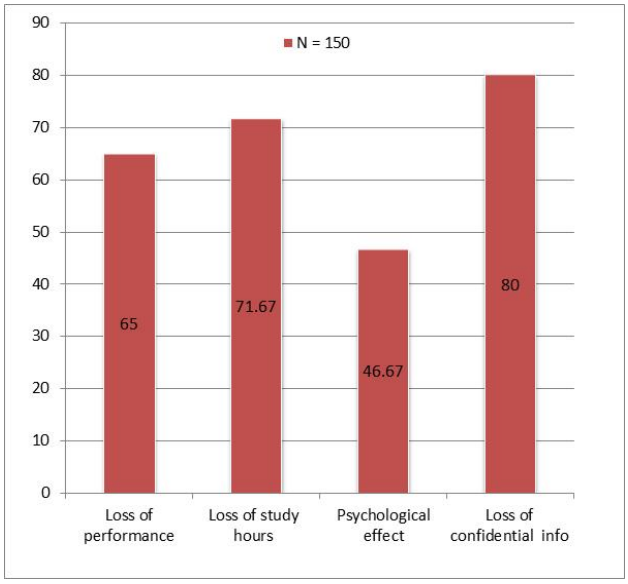

Figure 4. How the stakeholders (Students) are affected by m-learning security threats

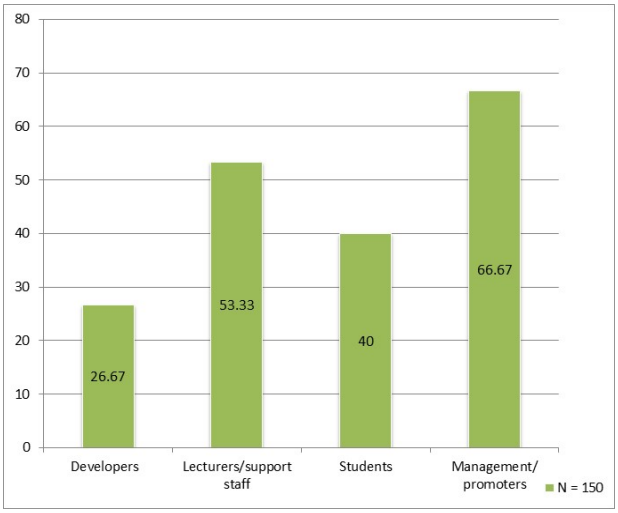

Figure 5. The affected stakeholders in m-learning

V. STATISTICAL ANALYSES

The Research Question One on m-learning security issues that stakeholders may face was analysed using Mann-Whitney U test for dependency based on the responses of the main stakeholders as shown in Table 1 and Table 2 below.

Table 1: Ranking of main stakeholders in m-learning security

Stakeholders	Participants	mean of ranks	sum of ranks
Students	120	10	50
Academics/support	30	4	28
Total	150	6.5	78

Table 2: Mann- Whitney test

Test	m-learning security threats
U Mann - Whitney	0 (critical value of u = 5)
Z	-2.7608
p-value (2-tailed)	0.05

According to Table 2, since the value of Z is less than -1.96 or greater than 1.96, **there is significant difference between students' and educators' perspectives in relation to the security issues that each set of stakeholders face in the use of m-learning.** This implies that the educators and students have different views on the m-learning security issues and they are being exposed to different risks which may be due their different use of mobile devices in education. While academic and support staff use their m-learning for teaching and passing knowledge, the students use their m-learning devices for learning. These different viewpoints are further explained in the discussion section.

Additionally, the Mann- Whitney U test was also performed on the data obtained on **Research Question Two regarding how the stakeholders in HEIs are affected by the security threats in m-learning**. The results of the statistical tests are shown 1n Table 3 and Table 4 below.

Table 3: Ranking of main stakeholders in m-learning

Stakeholders	Participants	mean of ranks	sum of ranks
Students	120	7	35
Academics/support	30	4	20
Total	150	5.5	55

Table 4: Mann- Whitney test

Test	m-learning security effects
U Mann - Whitney	5 (critical value of u = 2)
Z	-1.4623
p-value (2-tailed)	0.05

According to Table 4, **there is no significant difference between students and academic/ support staff viewpoints in relation to the security effects on stakeholders in m-learning**. This implies that both stakeholders are exposed to the same or similar security risks when using m-learning. This assertion is true because, being stakeholders, they both suffer loss of confidential information and privacy as well as psychological effects. In addition, academics and support staff may suffer loss of control over e-exams and content quality while the effect on students may include loss of study hours and performance.

VI. DISCUSSION

Fig. 1 illustrates security issues being encountered when using mobile devices for learning. Noticeable in the list is loss or theft of mobile devices. This is common in many developing countries since mobile devices are still

regarded as precious possessions and in some cases where the HEIs supplies learners with mobile devices, there are concerns about making learners attractive to thieves. This result is in line with the work of Obodoeze et al. [10] which identifies that the second most challenging security concern affecting mobile users in Nigeria is the frequent or widespread losses of mobile devices by their owners to thieves or by negligence. It is also consistent with a survey conducted by Jupiter [11] on mobile device users that showed that one out of every three mobile device users has lost their device at some point in time. Unauthorised access to learning content and interception of confidential information and personal details such as grades, feedback and emails by students and outsiders, either for fun or malicious acts, is a security threat which accounted for 75.6% and 45% respectively. Similarly, unpermitted sharing of copyrighted e-materials by the students among themselves is a security issue common among learners in HEIs in Nigeria. This is made possible due to inadequate copyright laws and software piracy in Nigeria [12, 13]. Virus and malware attacks are also threats to the use of handheld devices for learning purposes. This study also supports the work of Obodoeze et al. [10] who identify the various forms of threats including virus and malware attacks and hacking as the biggest security challenges being faced by mobile device users in Nigeria. Virus and malware threats are normally encountered when downloading educational materials from an unknown source. Propagation of false or misleading information using mobile devices among learners is a threat to m-learning. This is quite common as some students spread incorrect information through social media [14]. Denial of service is also a threat that usually affects the availability of m-learning system, mainly due to irregular power supply to mobile learning servers, a problem that is common in developing countries. This study is also consistent with the results of Osang et al. [15] in which 64% of the respondents identify that the poor power supply situation in Nigeria is a threat to m-learning.

How the educational institutions, educators and students are affected by m-learning security threats are shown in Figs. 2, 3 and 4 respectively. Common effect among all stakeholders is loss of confidential information, leading to loss of privacy. The study is consistent with the work of Kambourakis [2], who states that loss of confidential information is one of the worries for lecturers and their confidentiality should be guaranteed at all times. It is also consistent with the work of Zamzuri et al. [16] which states that one of the reasons why students reject online systems is due to security reasons because they are worried about the loss of their private and confidential information. Fig 3 indicates that the loss of control mainly during e-assessment and e-examination is a worry for the academic staff as this can lead to examination malpractices and unpermitted collaboration during assessments. This result is consistent with the study conducted by Osang et al. [15], in which most of the educators believed that m-learning will ease examination malpractices. Again, the findings agree with the work of Kambourakis [2], which revealed that e-examination procedures carried out in an unsupervised or semi-supervised way is one of the difficult challenges within the m-learning context. Therefore educators, who are interesting in using any technology for educational purposes, will want to take ownership and control of such projects [15]. Fig. 3 also shows that loss of content quality of learning materials is a likely side effect of introducing m-learning systems that can make it possible for learners to tamper with learning materials if the security is weak. Altering learning content and grades without authorisation from lecturers and amending confidential documents can be feasible if there is a security breach in the m-learning system known to the students.

Fig. 4 reveals that at least 60% of the students feared loss of study hours and performance as consequences of a security breach in m-learning due to denial of service. This is possible when learners have viewed m-learning as a complement to classroom and relied on it as a learning portal. Thus the non-availability of service for a long period of time will have adverse effects on learners' study hours, revision time and consequently their performance. This finding is in line with the work of Kukulska-Hulme et al. [17] which shows that good m-learning improves learners' study retention and performances in their study. Therefore, learners need a reliable, highly available and dependable m-learning system to avoid being frustrated when using the system, which can indirectly affect their study performance.

Research Question 4: What are the responsibilities of the stakeholders in ensuring risk free m-learning?

Having identified and discussed the m-learning security issues that stakeholders may face and how they are being affected by the security threats, it is important to note that the responsibility of ensuring a risk free m-learning environment lies mainly with the stakeholders themselves as they are the people involved in managing and using the system. Their collective responsibilities in ensuring risk free m-learning are highlighted in the recommendation section below.

VII. RECOMMENDATIONS

Based on the findings and results presented above and the cited literature, the following recommendations are the collective responsibilities of each specific stakeholder in ensuring risk a free m-learning environment.

Educational Institution/Management: The education providers have the main responsibilities of running risk free m-learning systems. The research findings indicate that 81.8% of the respondents agreed that the university management is responsible for ensuring risk free m-learning. This is expected as the university authority is the policy maker and also accountable for smooth running of the university facilities including m-learning infrastructures. herefore, the educational institutions/ promoters can ensure risk free m-learning by performing the following steps.

- Create security awareness among other stakeholders and encourage them to be security conscious when using their mobile devices. Educators and students should be made aware of the potential risk of connecting to bogus free Wi-Fi which criminals may have set up in public places in order to collect personal data. Creating security awareness is vital as our study revealed that some users do not take the security of their mobile devices very serious, so there is a need to promote mobile security education among users [19]. With adequate knowledge, students will be more security conscious about the safety of their handheld devices, thereby reducing the rate at which

small electronic gadgets are lost or stolen which is mainly due to their negligence.

- Implement separate wireless networks for academic users and visitors, to access the internet from their mobile devices whilst allowing restricted access to m-learning systems. This is to ensure that m-learning users have access only to their required or legitimate activities on the system and reduce unnecessary traffic to the servers.
- Implement mobile device management (MDM) systems for administering the m-learning devices in real-time, such as locate, track and gather information on the movement of devices, with the aim of remotely diagnosing and fixing software security problems, install and update software on devices and erase data on lost or stolen devices.
- In tackling the sharing of copyrighted e-materials, the university administrators can implement Digital Rights Management (DRM) solution. DRM is a technology that can be used for content protection in m-learning environment. It is a class of access control measures that are used to limit the use of digital content and devices. A DRM based m-learning system can focus on learning content protection and other basic procedures of m-learning facilities that can be secured.
- The university administrators can also operate a blacklisting method whereby websites or categories of websites deemed to be inappropriate or insecure are blocked from the university's network.

Academic staff: Around four out of ten (41%) of the respondents indicated that faculty lecturers are also responsible for ensuring risk free m-learning as they are in charge of running the academic programmes including the m-learning curriculum. The academic staff can ensure risk free m-learning through the following.

- Align the existing curriculum for m-learning with proper consideration for security as well as integrate new technology into their modules in a secure manner.
- Participate in the design and development of m-learning systems and mobile apps for their taught modules and research activities.
- Providing experts' opinions and contributions for the overall implementation and application of m-learning systems, in particular to their field of knowledge and research.
- Computer Science academic staff can develop a highly secured m-learning system following a standard security framework for implementation and participate in training the support staff on security concepts such as data encryption.

Developers/ Support staff: The responsibilities of support staff in ensuring risk-free m-learning include:

- Ensuring regular data backups are taken, installing firewalls on m-learning servers and having up to date anti-malware and anti-virus software installed on m-learning systems as well as installing all security patches.
- Putting in place proper security procedures and policies that will prevent hacking activities which may deny legitimate acts, a scheduled maintenance policy for m-learning servers and network infrastructure, as well as an uninterruptible power supply.

Students: In view of the students' concerns on m-learning, the following recommendations are offered for secure and effective m-learning.

- They should avoid connecting to unsecured public Wi-Fi as many of them connect to educational resources while on the move using any free available Wi-Fi. They should be aware of the credibility of the organisation providing the connection regarding the security and safety of free network facilitates before using it. For example, connecting to an unsecured and unverified wireless infrastructure increases the chances of putting personal data at risk.
- Security apps such as phone finders should be installed on mobile devices to enable locating them in case of lost or theft. Remote wipe apps should be installed to prevent unauthorised access to confidential and private information as well as learning materials stored on the devices if a lost device cannot be traced.

VIII. CONCLUSION

Until recently, stakeholders in education were unconcerned about security, mainly because users in academic fields tended to be non-malicious. Nowadays, security in learning environment is increasingly important because online learning applications and infrastructure have become 'business-critical' applications in HEIs [19]. Therefore, stakeholders, most especially the University management and academic staff are now seeing security issues in learning technologies as a part of the overall educational and business strategy of their institutions. Proper design of the technologies being used for online learning and adequate security management for m-learning system will lead to greater effectiveness, acceptability and usage of mobile learning [9]. The stakeholders of m-learning should focus not only on developing and using m-learning content and infrastructure but also make effort at securing the system because the users need a reliable, highly available and dependable m-learning system to avoid being frustrated when using the system.

REFERENCES

[1] S.A. Shonola and M.S. Joy (2014), 'Mobile learning security issues from lecturers' perspectives (Nigerian Universities Case Study)'. 6th International Conference on Education and New Learning Technologies, 7-9 July, 2014, Barcelona, Spain. pp. 7081-7088

[2] G. Kambourakis (2013). Security and Privacy in m-Learning and Beyond: Challenges and State of-the-art. International Journal of u- and e- Service, Science and Technology. Vol.6, no. 3, pp.67-84

[3] F. Graf (2002) 'Providing security for elearning'. Computers & Graphics. vol.26, no.2, pp.355–365 http://dx.doi.org/10.1016/S0097-8493(02)00062-6

[4] S.A Shonola and M.S Joy (2014), 'Mobile Learning Security Concerns from University Students' Perspectives'. 8th International Conference on Interactive Mobile Communication Technologies and Learning, November 13-14, 2014, Thessaloniki, Greece. pp. 165-172 http://dx.doi.org/10.1109/imctl.2014.7011125

[5] M. Guo, P. Bhattacharya, M. Yang, K. Qian, and L. Yang (2013). Learning mobile security with android security labware. In Proceeding of the 44th ACM technical symposium on Computer science education (pp. 675-680). ACM. http://dx.doi.org/10.1145/2445196.2445394

[6] A. Charlesworth (2009) "Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998", Tech.

rep., JISC Legal, (2009), [http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/DPACodeofpractice.pdf].

[7] M. Kamba (2009). Problems, challenges and benefits of implementing e-learning in Nigerian universities: An empirical study. International Journal of Emerging Technologies in Learning (IJET), vol. 4, no.1 http://dx.doi.org/10.3991/ijet.v4i1.653

[8] C.D.C Luminita and C.I.N Magdalena (2012). 'E-learning Security Vulnerabilities'. Procedia - Social and Behavioral Sciences 46 (2012) pp. 2297 – 2301 http://dx.doi.org/10.1016/j.sbspro.2012.05.474

[9] M. O. M El-Hussein and J.C Cronje (2010). 'Defining Mobile Learning in the Higher Education Landscape'. Educational Technology & Society, vol.13, no 3, pp. 12–2

[10] F.C. Obodoeze, F.A Okoye, C.N Mba, S.C. Asogwa and F.E. Ozioko (2013). A Holistic Mobile Security Framework for Nigeria. International Journal of Innovative Technology an Exploring Engineering (IJITEE), vol.2 , no.3, pp.1-11

[11] Juniper Networks (2012) '2011 Mobile threats report' Juniper Networks Inc, February, 2012

[12] K. M. Waziri (2011). Intellectual Property Piracy and Counterfeiting in Nigeria: The Impending Economic and Social Conundrum. Journal of Politics & Law vol. 4, no.2, pp.196-202 http://dx.doi.org/10.5539/jpl.v4n2p196

[13] B. A. Fabunmi (2009). The Roles of Librarians in Copyright Protection in Nigeria. International Journal of African & African-American Studies vol. 6, no.1, pp84-93

[14] P. O. Jegede (2009). Age and ICT-related behaviours of higher education teachers in Nigeria. Issues in Informing Science and Information Technology, vol.6, pp.770–777.

[15] B. F. Osang, J. Ngole and C. Tsuma (2013). Prospects and Challenges of Mobile Learning Implementation in Nigeria: Case Study National Open University of Nigeria (noun)'. A paper presented at International Conference on ICT for Africa 2013, February 20 -23, Harare, Zimbabwe

[16] Z. F. Zamzuri, M. Manaf, Y. Yunus, and A. Ahmad (2013). Student Perception on Security Requirement of e-Learning Services. Procedia-Social and Behavioral Sciences. 90(2013), pp.923-930. http://dx.doi.org/10.1016/j.sbspro.2013.07.169

[17] A. Kukulska-Hulme, M. Sharples, M. Milrad, I. Arnedillo-Sánchez and G. Vavoula (2009) 'Innovation in Mobile Learning: A European Perspective'. International Journal of Mobile and Blended Learning vol. 1, no. 1, pp. 13-35. http://dx.doi.org/10.4018/jmbl.2009010102

[18] S. Diaz (2012) 'Mobile security needs more than just software, needs education' Available online from http://www.zdnet.com/blog/btl/mobile-security-needs-more-than-just-software-needseducation/36437[Accessed on Jan 20, 2012].

[19] E. Weippl and M. Ebner, (2008). Security & Privacy Challenges in E-Learning 2.0. Proceedings of E-Learn 2008, Las Vegas, pp. 4001-4007

AUTHORS

S.A. Shonola is a PhD student and researcher at the Computer Science Department, University of Warwick, UK. (e-mail: s.a. shonola@ warwick.ac.uk).

M.S. Joy is an associate professor at the Computer Science Department, University of Warwick, UK. (e-mail: m.s. joy@ warwick.ac.uk).

This article is an extended and modified version of a paper presented at the International Conference of Interactive Mobile and Computer Aided Learning (IMCL2014), held in November 2014, in Thessaloniki, Greece. Submitted 15 February 2015. Published as resubmitted by the authors 18 May 2015.